UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,852	12/05/2003	Gregory A. Girsham	1505-0157	8312

7590 12/23/2008

Harold C. Moore
Maginot, Moore & Beck LLP
Bank One Center/Tower
111 Monument Circle, Suite 3000
Indianapolis, IN 46204-5115

EXAMINER	
WEST, THOMAS C	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,852	GIRSHAM ET AL.	
	Examiner	Art Unit	
	THOMAS WEST	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of the Application

1. This action is in response to the Arguments/Remarks filed September 2, 2008.

2. Claims 1-22 are pending and have been examined.

Response to Arguments

3. Applicant's arguments filed September 2, 2008 have been fully considered but they are not persuasive. Applicants argument regarding claims 2 and 14 involving the terms "arithmetically combines" and "arithmetically combining" is not supported by the specification, such as addition, subtraction, etc. Further arguments are moot in light of the new grounds of rejection.

Claim Rejections - 35 USC §101

4. 35 U.S.C. §101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 13-20 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Based on Supreme Court precedent and recent Federal Circuit decisions, § 101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a

different state or thing. If neither of these requirements is met by the claim(s), the method is not a patent eligible process under 35 U.S.C. § 101.

In this particular case, claim 13 and ITS dependent claims 14-20 lack sufficient technology. (Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780, 787-88 (1876)).

Claims 14-20 are also rejected as each depends from claim 13.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims1, 10, 13, 20, 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims 1, 10, 13, 20, 22 recite enabling a data access operation without reference to the security access tables. The claims and the specification do not describe how nor recite steps describing the "enabling" that avoids or circumvents the security access tables designed to prevent unauthorized data access.

8. Claims 1, 4, 6, 10, and 13-20, 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention. Claims 4 and 14 recite the terms "arithmetically combines" and "arithmetically combining" in claims 4 and 14 are relative terms which renders the claim indefinite. Both terms are not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Generation of the security key is rendered indefinite by the use of the above terms. Claims 6 and 15 recite the terms "augments" and "augmenting" are relative terms which render the claim indefinite. Both terms are not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Generation of the security key is rendered indefinite by the use of the above terms. Claims 13-20 recite "receiving a request", "generating a security key", "comparing an access key…", "enabling a data access operation", without describing who or what is receiving, generating, comparing, etc, rendering the claims indefinite. Further claims 1, 10, 13, 20, 22 recite enabling a data access operation without reference to the security access tables. The claims and the specification do not describe how nor recite steps describing the "enabling" that avoids or circumvents the security access tables designed to prevent unauthorized data access.

Claim Rejections - 35 USC § 103

9. Claims 1, 2-7, 13-15, 20-22 are rejected under U.S.C. 103(a) as being unpatentable over Germer, US Patent No. 7,065,457 in view of Matyas et al, US Patent

No. 4,918,728 in view of Haines, US Patent No. 5,107,455, and in further view of Kinter-Meyer, Utility/Energy Management and Control System Communication Protocol Requirements (Kinter-Meyer).

Examiner's Note: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

As per claims 1, 13, 20-22:

With regard to the limitation of *enabling a data access without reference to data table parameters*, Germer discloses: (col. 12, lines 38-50, data access, col. 2, lines 25-41, ANSI C12.19 standard tables)

Germer discloses the limitations above but does not disclose *a bypass component but Matyas does*. "Protection From Non-System Generated Keys. The method for coupling the control vector and key is such that CV checking is unable to detect a system generated key (via KGEN or GKS) from a non-system generated key. For this reason, a "back-door" method exists within the architecture for generating a keys and control vectors. It consists of defining a control vector "of choice" and a random number which is then represented as a key encrypted in the manner described under the architecture using the selected control vector. The so-called "back-door" method of key generation is primarily an annoyance, although in some cases cryptographic attacks would be possible if additional measures of defense were not taken in the architecture" (Matyas, column 15, lines 18-27 and 31-34, unable to detect a

system generated key (via KGEN or GKS) from a non-system generated key, back-door method).

The *Deacde4 table parameters* are the security limiting tables, which are part of the ANSI C12.19 standard where access permissions are used to limit table read or write access, although the exact means for granting access are not defined by the standard. The present invention involves a back-door or bypass method that goes around the ANSI C12.19 security features. Back-door or bypass security methods are well known in the art as exemplified by Maytas, which in this case, control vector checking is unable to detect a system generated key from a non-system generated key, much like what is being done in the current application.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer with the bypass of security features of Maytas since this allows for meter calibration and upgrade that would otherwise be denied access due to a data table read only restriction, incorporated by the ANSI C12.19 standard.

With regard to the limitation of security tables, Germer discloses ANSI C12.19 standard tables, but does not specifically disclose security tables, but Kinter-Meyer does (page 92)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer with the security tables of Kinter-Meyer in order to restrict data access operations.

Germer/Matyas disclose the limitations as shown above but do not disclose a security component, but Haines does:

a security component for determining whether an externally generated access key is the same as an internally generated access key (Haines, column 1, lines 67-68 and 2 lines 1-24, data center checks code, enable codes agree)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas with the security component of Haines in order to authenticate data access operations.

As per claims 13, 22:

Germer/Matyas disclose the limitations as shown above but do not disclose the following, but Haines does: *receiving a request for a security* key (Haines, column 1, lines 67-68 and 2 lines 1-24, I/O configuration request, data center)

Haines teaches: "The meter is reconfigured by first putting the meter into a I/O configuration mode by suitable entries from the keyboard. In this mode, the meter is inhibited from printing postage. The meter has a storage register for a current or old I/O configuration number (IOCN). A desired new IOCN is entered via keyboard entry. The meter software generates an encrypted I/O configuration request code that is partially based on the value of the new IOCN. The I/O configuration request code is communicated to a data center computer along with other validating identification information. The data center computer checks the code by computing the I/O configuration request code using the same algorithm. If the two values agree, the data center computer generates an encrypted I/O configuration enable code that is partially based on the meter serial number. This is communicated to the meter, which receives

the computer generated I/O configuration enable code and also generates an internal I/O configuration enable code using the same encryption algorithm as the data center computer. If the I/O configuration enable codes agree, the meter overwrites the old IOCN with the new IOCN in permanent storage. The external devices in communication with the meter may then read the IOCN and implement the feature set represented by the IOCN." (Haines, column 1, lines 67-68 and 2 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Maytas with the internally generated code of Haines to enhance security to prevent unauthorized data access operations.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas with the security key request of Haines since this requires user authentication prior to meter calibration and upgrade that would otherwise be denied access due to a data table read only restriction, incorporated by the ANSI C12.19 standard.

Germer/Matyas disclose the limitations as shown above but do not disclose the following, but Haines does:

generating a security key, Haines teaches, (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code),

generating an access key from the security key, wherein the generated access key is generated within the utility meter (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code, internal I/O configuration enable code)*;*

an access key generator configured to receive the security key and generate an internal access key (Haines, column 1, lines 67-68 and 2 lines 1-24)

comparing the generated access key to an externally generated access key (Haines, column 1, lines 67-68 and 2 lines 1-24, data center checks code, enable codes agree)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas with the sercurity key and access key generation and comparison Haines in order to prevent unauthorized meter access.

As per claims 2-6, 14, 15:

With regard to the limitations of, Germer/Matyas does not explicitly teach a security key generator, variable data, or augmenting an access key, but Haines does:

a security key generator for generating a security key (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code).

the security key generator generates the security key from variable data and data associated with the meter, Haines teaches (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code, column 3, lines 55-68 , col. 4, lines 1-9, meter serial number, CTID incremented (variable))

the security key generator arithmetically combines the variable data and the data associated with the meter to generate the security key, Haines explicitly teaches: (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code, column 3,

lines 55-68 , col. 4, lines 1-9, meter serial number, CTID incremented (variable), input numbers use to generate encrypted codes)

an access key generator for generating an access key from the security key, Haines explicitly teaches: *meter* (column 1, lines 67-68, column 2, lines 1-23, I/O configuration request code, internal I/O configuration enable code);.

the access key generator augments the security key before generating the access key, Haines explicitly teaches: (column 7, lines 58-68, column 8, lines 1-6, HSL value)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas with the security key generator, variable data, and augmenting an access key of Haines in order to further secure key generation from allowing fraudulent access.

As per claim 7:

With regard to the limitations of *an access key comparator for comparing the access key generated by the access key generator to an access key received from an external device,* Germer/Matyas does not explicitly teach this but Haines does (column 1, lines 67-68 and 2 lines 1-24, data center checks code, enable codes agree)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyasr with the access comparator of Haines in order to further secure key generation from allowing fraudulent access.

As per claim 21:

With regard to the limitation of *the standard meter industry data structures are ANSI C 12.19 data structures,* Germer discloses ANSI C 12.19 standard tables (col. 2, lines 25-41.

With regard to the limitation of the security data table parameters are Decade4 table parameters. Germer does not specifically disclose the above but Kinter-Meyer does (see pages 92, 162).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas/Haines with the ANSI C 12.19 security tables of Kinter-Meyer since the ANSI C 12.19 standard includes restricted access to read-only tables through the use of the security tables.

10. Claims 8-12, 16-19 are rejected under U.S.C. 103(a) as being unpatentable over Germer, US Patent No. 7,065,457 in view of Matyas et al, US Patent No. 4,918,728 in view of Haines, US Patent No. 5,107,455, in further view of Kinter-Meyer, Utility/Energy Management and Control System Communication Protocol Requirements (Kinter-Meyer) and in further view of Hoffman et al, US Patent No. 5, 715, 390.

As per claims 8-12, 16, 17:

Germer/Matyas/Haines/Kinter does not explicitly teach an access monitor, unlock timer, single data access, and procedures, but Hoffman does:

a data access monitor for monitoring data access operations performed by the external device and resetting the access key comparator in response to a data access being performed by the external device. Hoffman explicitly teaches: "In accordance with the present invention, ROM includes codes for implementing one or more stored options or upgrades. It will be appreciated that these options or upgrades are stored in the meter at the factory and can be utilized only when purchased and enabled as described herein. Each meter has a unique serial number stored in RAM. In the present example, the serial number is 16 bytes long and includes bit-flags (i.e., an option byte) indicating which options have already been enabled. Each option which is not enabled must be requested and a password verified before it can be utilized. It is an important feature of the present invention that the password be based on the serial number, so that the same password cannot simply be recorded and played back to another meter. Further, the password cannot be used to upgrade more than the option(s) selected (and purchased) " (Hoffman, column 2 lines 16-29).

"The upgrade command initiates the ROM codes for implementing one or more stored options or upgrades in step 81. The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program." (Hoffman, column 4, lines 61-65).

"After 330 cycles, the contents of bytes B30, B31, B32, and B33 are defined to be the password corresponding to the specific key, meter serial number, and option. The authentication algorithm being known will not in of itself allow recovery of the secret key. Further, if a single bit is changed in the serial number, the option byte, or the key,

then the authentication password will change in a difficult to predict fashion" (Hoffman, column 5, lines 46-54).

"It will be appreciated that the change in the option status has resulted in a significant change in the password. This is also the case for a small change in the serial number or the key" (Hoffman, column 6, lines 3-6).

It is clear from the references above that the upgrade command and the counter function as a data access monitor since each option which is not enabled must be requested and a password verified before it can be utilized. The authentication algorithm referenced above functions as the reset mechanism since it prevents further upgrades through a significant change in the password should any small change occur in the option status, key, or serial number of the meter. A change in this externally generated password would not match the meter's internally generated password preventing further data access to the meter, functioning as reset of the access key comparator of the current invention.

With regard to the limitations of *a unlock timer for timing an interval corresponding to a data access operation and for resetting the access key comparator in response to a data access being performed by the external device*. Hoffman explicitly teaches: "The counter is decremented each time an upgrade is downloaded to a meter, so that only the number of upgrades purchased can be enabled" (Hoffman, column 4, lines 65-67).

The counter above functions as an unlock timer providing limited data access for a period based on the number of upgrades purchased that can be enabled. As mentioned above, the authentication algorithm functions as the reset mechanism since it prevents further upgrades through a significant change in the password should any small change occur in the option status, key, or serial number of the meter.

With regard to the limitations of the bypass component enables a single data access operation by the external device. Hoffman explicitly teaches: "The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program" (Hoffman, column 2, line 62-64).

"The password is generated by processing a software key and a serial number of the meter with an authentication program by a processor external to the meter" (Hoffman, column 4, lines 47-50).

The upgrade software program above sends a command identifying the desired option, which enables a data access operation for upgrading the meter through an external device (Hoffman, column 2, lines 62-64).

"The counter is decremented each time an upgrade is downloaded to a meter, so that only the number of upgrades purchased can be enabled" (Hoffman, column 4, lines 65-67).

It should be clear from the above references, that the counter above functions as an unlock timer providing limited data access for a period based on the number of

upgrades purchased that can be enabled and that upgrading is done through an external device.

With regard to the limitations of *the security component and bypass component are implemented by a procedure*. Hoffman explicitly teaches: "The upgrade command identifying the desired option or upgrade is programmed into the upgrade software program" (Hoffman, column 4, line 63-65).

- The security component and the upgrade software program are equivalent per Claim 2's rejection and it is well known in the art that software programs contain and are developed through the use of procedures.
- The bypass component and the upgrade software program are equivalent per Claim 1's rejection and it is well known in the art that software programs contain and are developed through the use of procedures.

With regard to the limitations of *the procedure is a computer program executed by a processor in the utility meter*. Hoffman explicitly teaches: "The password along with an upgrade command are presented to the meter where they are compared to the read-protected passwords in the RAM of the meter, and, if there is a match, then the upgrade command initiates the ROM codes for implementing one or more stored options or upgrades (Hoffman, column 4, lines 57-63).

The comparison of passwords is obviously done, to someone skilled in the art, by the meter's internal processor and the processor also responds thereafter to the upgrade command.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas/Haines/Kinter with the access monitor, unlock timer, single data access, and procedures of Hoffman in order to further secure data access from fraudulent procedures.

As per claims 18, 19:

Germer/Matyas/Haines/Kinter does not explicitly teach the following limitations, but Hoffman does:

generating the access key with an encryption function,

Hoffman explicitly teaches: "After 330 cycles, the contents of bytes B30, B31, B32, and B33 are defined to be the password corresponding to the specific key, meter serial number, and option. The authentication algorithm being known will not in of itself allow recovery of the secret key. Further, if a single bit is changed in the serial number, the option byte, or the key, then the authentication password will change in a difficult to predict fashion" (Hoffman, column 5, lines 47-54).

The authentication algorithm being known does not in and of itself allow recovery of the secret key, is indicative of and the result of, to on skilled in the art, to an encryption function.

generating the access key with a hashing function.

Hoffman explicitly teaches: It will be appreciated that the change in the option status has resulted in a significant change in the password. This is also the case for a small change in the serial number or the key." (Hoffman, column 6, lines 3-6).

This result is indicative of and the result of, to one skilled in the art, to a hashing function, where the fundamental property of all hash functions is that if two hashes, according to the same function, are different, then the two inputs are different in some way.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Germer/Matyas/Haines/Kinter with the encryption and hashing functions of Hoffman in order to further secure data access from fraudulent procedures.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas West whose telephone number is 571-270-1236. The examiner can normally be reached on Tuesday and Wednesday 7:30am - 5pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thomas West
Patent Examiner
Art Unit 3621
December 17, 2008

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621